ELSEVIER

Theoretical Computer Science 276 (2002) 133–146

Theoretical Computer Science

www.elsevier.com/locate/tcs

Cryptographically significant Boolean functions with five valued Walsh spectra

Subhamoy Maitra[a,*], Palash Sarkar[b]

[a]*Computer & Statistical Service center, Indian Statistical Institute, 203 B. T. Road, Calcutta 700 035, India*

[b]*Applied Statistics Unit, Indian Statistical Institute, 203 B. T. Road, Calcutta 700 035, India*

Received July 2000; received in revised form February 2001; accepted March 2001

Communicated by A. Salomaa

Abstract

We describe methods to construct balanced (resp. 1-resilient) functions of odd number of variables n achieving the bent concatenation nonlinearity and having algebraic degree $n-1$ (resp. $n-2$). The technique is to algebraically modify the concatenation of two properly chosen $(n-1)$-variable Maiorana–McFarland bent functions. The constructed functions can be used with certain recursive operators to provide higher order resilient functions with maximum possible degree and high nonlinearity. Such functions are well suited for stream cipher applications. Interestingly, all the constructed functions have a five valued Walsh spectra.

Keywords: Boolean function; Balancedness; Nonlinearity; Bent function; Algebraic degree; Correlation immunity; Resiliency; Stream cipher

1. Introduction

Boolean functions are used as nonlinear combining functions in certain models of stream ciphers. Such a function should possess certain desirable properties to withstand the known cryptanalytic attacks. Four such important properties are balancedness, correlation immunity, algebraic degree and nonlinearity (see definitions in Section 2). Among these, nonlinearity is perhaps the most combinatorially challenging property.

* Corresponding author.

E-mail addresses: subho@isical.ac.in (S. Maitra), palash@isical.ac.in (P. Sarkar).

0304-3975/02/$ - see front matter

PII: S0304-3975(01)00196-7

The maximum possible nonlinearity for n-variable functions is known only for even n and equals $2^{n-1} - 2^{(n-2)/2}$. Functions achieving this nonlinearity are called bent and were introduced by Rothaus [14]. Later work have produced various characterizations and constructions of bent functions [4, 3, 2].

When the number of variables n is odd, an easy way to obtain high nonlinearity is to concatenate two bent functions on $(n-1)$ variables. The value of nonlinearity achieved is $2^{n-1} - 2^{(n-1)/2}$ and is called the bent concatenation nonlinearity. It is known that for $n \leqslant 7$, this is the maximum possible nonlinearity. For $n \geqslant 9$, the maximum value of nonlinearity is not known, though there are some upper bounds [8]. Also Patterson and Weidemann [12, 13], showed that for odd $n \geqslant 15$ it is possible to construct functions with nonlinearity higher than the bent concatenation value. It is of interest to construct functions achieving the bent concatenation nonlinearity and possesing other cryptographic properties [5].

In this paper we first concentrate on functions on odd number of variables achieving the bent concatenation nonlinearity. We show that it is possible to construct such functions which are

- balanced and have the maximum possible degree $n-1$,
- balanced, correlation immune of order 1 and have the maximum possible degree $n-2$.

Our technique is to modify a well-known construction of bent functions, the Maiorana–McFarland construction, to achieve the above properties. Further, we use these functions along with certain recursive operators to construct higher order resilient functions with maximum possible degree and very high nonlinearity. These functions are well suited for stream cipher applications. It is interesting to note that all the constructed functions have a five valued Walsh spectrum.

2. Preliminaries

In this section we introduce a few basic concepts. Note that we denote the addition operator over $GF(2)$ by $\oplus$. By Ω_n we denote the set of n-variable Boolean functions.

Definition 1. Let s, s_1, s_2 be binary strings of same length λ.

- The bitwise complement (resp. reverse) of s is denoted by s^c (resp. s^r). The string s^{rc} denotes complemented reversal of the string s.
- We denote by $\#(s_1 = s_2)$ (resp. $\#(s_1 \neq s_2)$), the number of places where s_1 and s_2 are equal (resp. unequal).
- The Hamming distance between s_1, s_2 is denoted by $d(s_1, s_2)$, i.e. $d(s_1, s_2) = \#(s_1 \neq s_2)$.
- The Walsh Distance $wd(s_1, s_2)$, between s_1 and s_2, is defined as, $wd(s_1, s_2) = \#(s_1 = s_2) - \#(s_1 \neq s_2)$. Note that, $wd(s_1, s_2) = \lambda - 2d(s_1, s_2)$.
- The Hamming weight or simply the weight of s is the number of ones in s and is denoted by $wt(s)$.
- An n-variable function f is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e. $wt(f) = 2^{n-1}$).

An n-variable Boolean function $f(X_n,\ldots,X_1)$ can be uniquely represented by a multivariate polynomial over $GF(2)$.

Definition 2. Let $f(X_n,\ldots,X_1)$ be an n-variable function. We can write

$$f(X_n,\ldots,X_1) = a_0 \oplus \left(\bigoplus_{i=1}^{i=n} a_i X_i\right) \oplus \left(\bigoplus_{1\leqslant i\neq j\leqslant n} a_{ij}X_iX_j\right) \oplus \cdots \oplus a_{12\ldots n}X_1X_2\ldots X_n,$$

where the coefficients $a_0, a_{ij},\ldots,a_{12\ldots n} \in \{0,1\}$. This representation of f is called the algebraic normal form (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of f.

Functions of degree at most one are called affine functions. An affine function with constant term equal to zero is called a linear function. The set of all n-variable affine (resp. linear) functions is denoted by $A(n)$ (resp. $L(n)$). The relation between Hamming distance and Walsh distance of two linear functions is given in the following result.

Proposition 3. *Given* $l_1, l_2 \in L(k)$, $d(l_1,l_2) = 0, 2^{k-1}, 2^k$ $(wd(l_1,l_2) = 2^k, 0, -2^k)$ *accordingly as* $l_1 = l_2$, $l_1 \neq l_2$ *or* $l_2^c, l_1 = l_2^c$.

Definition 4. The nonlinearity $nl(f)$ of an n-variable function f is defined as

$$nl(f) = \min_{g\in A(n)} (d(f,g)),$$

i.e. $nl(f)$ is the distance of f from the set of all n-variable affine functions.

An important tool for the analysis of Boolean function is its Walsh transform, which we define next [6].

Definition 5. Let $f(\bar{X})$ be an n-variable Boolean function. Let us consider $\bar{X} = (X_n,\ldots,X_1)$ and $\bar{\omega} = (\omega_n,\ldots,\omega_1)$ both belong to $\{0,1\}^n$ and $\langle \bar{X}, \bar{\omega}\rangle = X_n\omega_n \oplus \cdots \oplus X_1\omega_1$. Then the Walsh transform of $f(\bar{X})$ is a real valued function over $\{0,1\}^n$, which is defined as

$$W_f(\bar{\omega}) = \sum_{\bar{X}\in\{0,1\}^n} (-1)^{f(\bar{X})\oplus\langle\bar{X},\bar{\omega}\rangle}.$$

The Walsh transform is sometimes called the spectral distribution or simply the spectrum of a Boolean function.

A function f of $2k$ variables is called bent if $W_f(\bar{\omega}) = \pm 2^k$ for all $\bar{\omega} \in \{0,1\}^{2k}$. These functions are important in both cryptography and coding theory since they achieve the maximum possible nonlinearity. One simple way to construct a bent function on $2k$ variables is the following [14]. Consider the set $A(k)$ of all affine functions on k variables. Each of these functions can be represented by a bit string of length 2^k, the

output column of the truth table. Let $f = f_1 \dots f_{2^k}$ be a concatenation of 2^k functions from $A(k)$ such that for $i \neq j$, $f_i \neq f_j$ or f_j^c. Then it can be shown that f is a bent function. These bent functions are called the Maiorana–McFarland bent functions. Later we will use suitable bent functions of this type to construct our functions.

Correlation immune functions were introduced by Siegenthaler [15], to withstand a class of "divide-and-conquer" attacks on certain models of stream ciphers. Xiao and Massey [7] provided a spectral characterization of correlation immune functions. Here we state this characterization as the definition of correlation immunity.

Definition 6. A function $f(X_n,\dots,X_1)$ is mth order correlation immune (CI) iff its Walsh transform W_f satisfies

$$W_f(\bar{\omega}) = 0 \quad \text{for } 1 \leqslant wt(\bar{\omega}) \leqslant m.$$

Further, if f is balanced then $W_f(\bar{0}) = 0$. Balanced mth order correlation immune functions are called m-resilient functions.

Thus, a function $f(X_n,\dots,X_1)$ is m-resilient iff its Walsh transform W_f satisfies

$$W_f(\bar{\omega}) = 0 \quad \text{for } 0 \leqslant wt(\bar{\omega}) \leqslant m.$$

The relationship between Walsh transform and Walsh distance is $W_f(\bar{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i)$.

3. Balanced functions

We first provide a construction of n-variable balanced function (n odd) with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and algebraic degree $(n-1)$.

Theorem 7. *For odd $n \geqslant 3$, it is possible to construct balanced $f \in \Omega_n$, with algebraic degree $(n-1)$ and nonlinearity $2^{n-1} - 2^{(n-1)/2}$.*

Proof. For $n = 3$, the function $f(X_3,X_2,X_1) = X_3 \oplus X_1X_2$ satisfies the condition. The construction for $n \geqslant 5$ is the following. Let $n = 2k+1$ and $r = 2^k$. Let $h_1, h_2 \in \Omega_{2k}$ be Maiorana–McFarland bent functions of the following form. The function h_1 is a concatenation of 2^k distinct linear functions of k variables, where the first linear function is the all zero function. The function h_2 is same as h_1 except the first function is the all one function in place of the all zero function. Thus, the binary strings are of the form $h_1 = 0^r\lambda$ and $h_2 = 1^r\lambda$, where λ is a binary string of length $2^{2k} - 2^k$, a concatenation of $2^k - 1$ distinct nonconstant linear functions of k variables. Note that 0^x (resp. 1^x) denotes the all zero (resp. all one) string of length x. Next we construct $h_1' = 10^{r-1}\lambda$ and $h_2' = 01^{r-1}\lambda$ by complementing the first bit of both h_1, h_2. In algebraic terms the

construction of h'_1 and h'_2 can be described as follows:

$$h'_1(X_{n-1},\ldots,X_1) = h_1(X_{n-1},\ldots,X_1) \oplus (1 \oplus X_{n-1})\ldots(1 \oplus X_1),$$

$$h'_2(X_{n-1},\ldots,X_1) = h_2(X_{n-1},\ldots,X_1) \oplus (1 \oplus X_{n-1})\ldots(1 \oplus X_1).$$

We define

$$f(X_n,\ldots,X_1) = (1 \oplus X_n)h'_1(X_{n-1},\ldots,X_1) \oplus X_n h'_2(X_{n-1},\ldots,X_1),$$

i.e., $f = h'_1 h'_2$, the concatenation of strings h'_1 and h'_2. Note that f is of the form $10^{r-1}\lambda 01^{r-1}\lambda$. Also note that

$$wt(f) = wt(h'_1) + wt(h'_2) = wt(h_1) - 1 + wt(h_2) + 1 = 2^{n-2} + 2^{n-2} = 2^{n-1}.$$

Thus f is balanced. Since, both $wt(h'_1), wt(h'_2)$ are odd, f is of algebraic degree $(n-1)$. Next we calculate the nonlinearity of f. For this we have to compute distance of f from the set of affine functions $A(n)$. Any linear function in $L(n)$ is of the form ll or ll^c, for some $l \in L(n-1)$. So we have two cases.

Case 1: We first consider linear functions of the form $ll \in L(n)$, where $l \in L(n-1)$. We write $l = l_x l_y$, where l_x is a binary string of length 2^k and l_y is a binary string of length $2^{2k} - 2^k$. Now,

$$\begin{aligned} d(f, ll) &= d(10^{r-1}\lambda 01^{r-1}\lambda, l_x l_y l_x l_y) \\ &= d(10^{r-1}, l_x) + d(\lambda, l_y) + d(01^{r-1}, l_x) + d(\lambda, l_y) \\ &= d(10^{r-1}, l_x) + d(01^{r-1}, l_x) + 2d(\lambda, l_y). \end{aligned}$$

Since, 10^{r-1} and 01^{r-1} are bitwise complements, $d(10^{r-1}, l_x) + d(01^{r-1}, l_x) = 2^k$. Now consider $d(\lambda, l_y)$. We represent $\lambda = \lambda_1\lambda_2\ldots\lambda_p$ and $l_y = l_1 l_2 \ldots l_p$, where $p = r - 1 = 2^k - 1$ and $\lambda_i,\ l_i \in A(k)$. Further each l_i is equal to μ or μ^c for some $\mu \in L(k)$. This gives rise to three conditions as follows:

(1) $l_i = \lambda_i$ for some i, $1 \leqslant i \leqslant p$. Then $l_j \neq \lambda_j$ or λ_j^c for all $j \neq i$, $1 \leqslant j \leqslant p$. From Proposition 3, we have $d(l_j, \lambda_j) = 2^{k-1}$ for $j \neq i$. The distance is contributed from the $2^k - 2$ slots, whereas one slot for index i contributes no distance. So, $d(\lambda, l_y) = (2^k - 2) \times 2^{k-1}$. This gives, $2d(\lambda, l_y) = 2^{2k} - 2 \times 2^k$. Hence,

$$d(f, ll) = 2^k + 2^{2k} - 2 \times 2^k = 2^{2k} - 2^k. \tag{I}$$

(2) $l_i = \lambda_i^c$ for some i, $1 \leqslant i \leqslant p$. Again $l_j \neq \lambda_j$ or λ_j^c for all $j \neq i$, $1 \leqslant j \leqslant p$. The distance is contributed from the $2^k - 2$ slots, and also the slot for index i which contributes distance of 2^k. Then $d(\lambda, l_y) = (2^k - 2) \times 2^{k-1} + 2^k$, i.e. $2d(\lambda, l_y) = 2^{n-1} - 2 \times 2^k + 2 \times 2^k$. Thus,

$$d(f, ll) = 2^{2k} + 2^k. \tag{II}$$

(3) $l_j \neq \lambda_j$ or λ_j^c for all $1 \leqslant j \leqslant p$.

Then $d(\lambda, l_y) = (2^k - 1) \times 2^{k-1}$, i.e. $2d(\lambda, l_y) = 2^{2k} - 2^k$. Thus,

$$d(f, ll) = 2^{2k}. \tag{III}$$

Case 2: Next we consider linear function of the form $ll^c \in L(n)$, where $l \in L(n-1)$. Now, $d(f, ll^c) = d(10^{2^k-1}, l_x) + d(\lambda, l_y) + d(01^{2^k-1}, l_x^c) + d(\lambda, l_y^c)$. Note that $l_x \in L(k)$. Since, 10^{r-1} and 01^{r-1} are bitwise complements, $d(10^{r-1}, l_x) + d(01^{r-1}, l_x^c) = 2 \times d(10^{r-1}, l_x) = 2$ or $2^k + 2$. Also, $d(\lambda, l_y) + d(\lambda, l_y^c) = 2^{2k} - 2^k$. Hence, we get two possible distances,

$$d(f, ll^c) = 2^{2k} - 2^k + 2, \tag{IV}$$

$$d(f, ll^c) = 2^{2k} + 2. \tag{V}$$

Thus, for $l \in L(n-1)$, $2^{2k} - 2^k \leqslant d(f, ll), d(f, ll^c) \leqslant 2^{2k} + 2^k$, and consequently for any affine function $v \in A(n)$, $2^{2k} - 2^k \leqslant d(f, v) \leqslant 2^{2k} + 2^k$. Hence, $nl(f) = 2^{2k} - 2^k = 2^{n-1} - 2^{(n-1)/2}$. □

From (I)–(V) above we get the following.

Corollary 8. *For odd $n \geqslant 5$, any function constructed using Theorem 7, has a five valued spectrum.*

Proof. Considering the values of distances, the Walsh spectrum of these functions contains the distinct values $\pm 2^{(n+1)/2}, 0, (2^{(n+1)/2} - 4), -4$. □

For $n = 3$, the Walsh spectrum for the Boolean function $f(X_3, X_2, X_1) = X_3 \oplus X_1X_2$ contains only three values $0, \pm 4$, and hence is not five valued.

Next we present a construction of n-variable balanced function (n odd) with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and algebraic degree $(n-2)$. This will be later used in the construction of 1-resilient functions.

Theorem 9. *For odd $n \geqslant 5$, it is possible to construct balanced $f \in \Omega_n$, with algebraic degree $(n-2)$ and nonlinearity $2^{n-1} - 2^{(n-1)/2}$.*

Proof. As before let $n = 2k + 1$ and $r = 2^k$. We consider a $2k$-variable bent function h_1 of the form $h_a h_b h_c$, where

- h_a is the all zero string of length 2^k,
- h_b is of length $2^{2k} - 2 \times 2^k$ and is a concatenation of $2^k - 2$ distinct degenerate nonconstant linear functions of k variables, and
- h_c in $L(k)$ is the linear function which is nondegenerate on all the k variables.

We complement the first and last bits of h_1, i.e. the first bit of h_a and the last bit of h_c. This gives a function h_1' in Ω_{2k} which is of the form xyz, where x is obtained from h_a by complementing the first bit, y is h_b and z is obtained from h_c by complementing the last bit. Define h_2' to be $x^c yz^c$. We define f to be the concatenation $xyzx^c yz^c$,

i.e., $h'_1 h'_2$. In other words,

$$h'_1(X_{2k},\ldots,X_1) = h_1(X_{2k},\ldots,X_1) \oplus (1 \oplus X_{2k})\ldots(1 \oplus X_1) \oplus X_{2k}\ldots X_1,$$

$$h'_2(X_{2k},\ldots,X_1) = h'_1(X_{2k},\ldots,X_1) \oplus (1 \oplus X_{2k})\ldots(1 \oplus X_{k+1}) \oplus X_{2k}\ldots X_{k+1}.$$

Then,

$$f(X_n,\ldots,X_1) = (1 \oplus X_n)h'_1(X_{n-1},\ldots,X_1) \oplus X_n h'_2(X_{n-1},\ldots,X_1).$$

First note that f is balanced since $wt(f) = (wt(x) + wt(x^c)) + (2 \times wt(y)) + (wt(z) + wt(z^c)) = (2^{(n-1)/2}) + (2^{n-1} - 2 \times 2^{(n-1)/2}) + (2^{(n-1)/2}) = 2^{n-1}$.

Write f as a concatenation $f_1 f_2 f_3 f_4$, where each $f_i \in \Omega_{n-2}$. Then $f_1 = xy_1$, $f_2 = y_2 z$, $f_3 = x^c y_1$ and $f_4 = y_2 z^c$, where $y = y_1 y_2$ with length of y_1 equal to length of y_2. Also it is easy to see that $wt(y_1)$ and $wt(y_2)$ are both even since these are formed by concatenating nonconstant affine functions. Further, $wt(x), wt(z), wt(x^c), wt(z^c)$ are all odd and hence $wt(f_i)$ is odd for all $1 \leqslant i \leqslant 4$. From this we get that the algebraic degree of f is at least $n-2$. Moreover, by expanding the algebraic normal form of f, it can be seen that all terms of degree $n-1$ vanish. Thus the degree of f is $n-2$.

The proof for nonlinearity is similar to that of Theorem 7. The different values of distance between f and linear functions from $L(n)$ are $2^{n-1} \pm 2^{(n-1)/2}, 2^{n-1}, 2^{n-1} - 2^{(n-1)/2} + 4$, $2^{n-1} + 4$. Hence the nonlinearity of f is $2^{n-1} - 2^{(n-1)/2}$. □

Corollary 10. *For odd $n \geqslant 7$, the functions constructed by Theorem 9 have five valued spectra.*

Proof. Considering the values of distances, the Walsh spectrum of these functions contains the distinct values $\pm 2^{(n+1)/2}, 0, 2^{(n+1)/2} - 8, -8$. □

Note that for $n = 5$ the function constructed in Theorem 9 has only a three valued spectrum $0, \pm 8$.

4. Resilient functions

We use the results of the previous section to first construct 1-resilient functions. Using these as initial functions and some recursive operators we provide a simple method to construct m-resilient functions with very high nonlinearity.

Theorem 11. *For all even $n \geqslant 4$, it is possible to construct 1-resilient functions with degree $n-2$ and nonlinearity $2^{n-1} - 2^{n/2}$.*

Proof. Let $f \in \Omega_{n-1}$ be constructed using Theorem 7. Then f is a balanced function of degree $n-2$ and nonlinearity $2^{n-2} - 2^{(n-2)/2}$. Let

$$g(X_n,\ldots,X_1) = X_n \oplus f(X_{n-1},\ldots,X_1)$$

and

$$h(X_n,\ldots,X_1) = (1 \oplus X_n) f(X_{n-1},\ldots,X_1) \oplus X_n f(1 \oplus X_{n-1},\ldots,1 \oplus X_1).$$

Then it is known [1, 10] that both g and h are n-variable, 1-resilient functions having degree $n-2$ and nonlinearity $2^{n-1} - 2^{n/2}$. □

For odd n, we use a different method to obtain 1-resilient functions. Given a function $f \in \Omega_n$, we define

$$S_f = \{\bar{\omega} \in \{0,1\}^n \mid W_f(\bar{\omega}) = 0\}.$$

If there exist n linearly independent vectors in S_f, then we can construct a nonsingular $n \times n$ matrix B_f whose rows are linearly independent vectors from S_f. Let, $C_f = B_f^{-1}$. Now define

$$f'(\bar{X}) = f(C_f \bar{X}).$$

Both f' and f *have the same weight, nonlinearity and algebraic degree* [9]. Moreover,

$$W_{f'}(\bar{\omega}) = 0$$

for $wt(\bar{\omega}) = 1$. This ensures that f' is CI of order 1. Further if f is balanced then f' is 1-resilient.

This technique has been used in [11]. However, they started with a random Boolean function and hence could not obtain a nonlinearity of $2^{n-1} - 2^{(n-1)/2}$. Here we start with an n-variable balanced function constructed by Theorem 7, having degree $(n-2)$ and nonlinearity $2^{n-1} - 2^{(n-1)/2}$. Since these parameters are preserved by a linear transformation on the variables, we obtain 1-resilient, n-variable function with degree $(n-2)$ and nonlinearity $2^{n-1} - 2^{(n-1)/2}$. We now show that it is always possible to obtain such a linear transformation.

Let e_i^n be an n-bit vector with ith $(1 \leqslant i \leqslant n)$ entry 1 and all other entries 0. For example $\mathrm{e}_n^n = (1,0,\ldots,0)$ and $\mathrm{e}_1^n = (0,\ldots,0,1)$.

For $n \equiv 3 \bmod 4$, define

$$r_1 = \mathrm{e}^n_{\frac{n-1}{2}} \oplus \cdots \oplus \mathrm{e}_1^n,$$

$$r_i = \mathrm{e}^n_{n+1-i}, \quad 2 \leqslant i \leqslant \frac{n+1}{2}$$

and

$$r_i = \mathrm{e}_n^n \oplus \left(\bigoplus_{1 \leqslant j \leqslant \frac{n-1}{2},\, j \neq n+1-i} \mathrm{e}_j^n \right), \quad \frac{n+1}{2} + 1 \leqslant i \leqslant n.$$

For $n \equiv 1 \bmod 4$, define

$$r_1 = e_1^n \oplus e_2^n \oplus e_{n-1}^n \oplus e_n^n,$$

$$r_i = e_{n+1-i}^n, \quad 2 \leqslant i \leqslant \frac{n+1}{2}$$

and

$$r_i = e_n^n \oplus e_{n+1-i}^n, \quad \frac{n+1}{2} + 1 \leqslant i \leqslant n.$$

Let B_n be a matrix whose rows are $r_1, \ldots, r_n$.

Example 12. In this example we provide B_7 and B_9.

$$B_7 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad B_9 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The following result follows from the definition of B_n.

Proposition 13. *The matrix B_n is nonsingular. Moreover, for $n \equiv 3 \bmod 4$, B_n is symmetric and is its own inverse.*

Proof. We first prove the case for $n \equiv 1 \bmod 4$. Let S be a subset of rows of B_n. If $r_1 \notin S$, then clearly S is linearly independent. So suppose that $r_1 \in B_n$. Note that in B_n, the submatrix formed by dropping the first two and last two rows and the first two and the last two columns is the identity matrix I_{n-4}. Hence, the inclusion or exclusion of the rows r_3 to r_{n-2} in S do not affect the linear independence of S. Hence, we assume that these rows are not in S. Thus S contains r_1 and a subset of $\{r_2, r_{n-1}, r_n\}$. Let x be the n-bit vector formed from the linear combination of the vectors in S. If both $r_n, r_{n-1} \in S$ or both $r_n, r_{n-1} \notin S$, then the first bit of x is 1. On the other hand, if r_n (resp. r_{n-1}) is not in S, then the nth bit (resp. the $(n-1)$th bit) of x is 1. Thus in all cases $x \neq 0$.

In the case $n \equiv 3 \bmod 4$, it is easy to check from the definition that B_n is symmetric. We prove that (1) the weight of any row of B_n is odd and (2) the rows of B_n are pairwise orthogonal. This will prove that B_n is nonsingular and is its own inverse. Again from the definition of B_n, it follows that the weight of each row is odd. Thus the inner product of a row with itself is 1. We now show that any two distinct rows are orthogoal. Let r_i, r_j be two distinct rows of B_n. If either of $i, j \in \{2, \ldots (n+1)/2\}$,

then clearly the inner product of r_i, r_j is 0. So suppose that both $i, j \notin \{2, \ldots (n+1)/2\}$. If both $i, j \in \{(n+1)/2+1, \ldots, n\}$, then the weight w_{ij} of $r_i \oplus r_j$ is 2. Let d_{ij} be the number of places where both r_i and r_j are 1. Then $w_{ij} = wt(r_i) + wt(r_j) - 2d_{ij}$. Since both $wt(r_i)$ and $wt(r_j)$ are odd and $wt(r_i) = wt(r_j)$, we have $wt(r_i) + wt(r_j) \equiv 2 \bmod 4$. Further, since $w_{ij} = 2$, it follows that $w_{ij} - (wt(r_i) + wt(r_j)) \equiv 0 \bmod 4$ and hence d_{ij} is even. The inner product of r_i and r_j is the parity of d_{ij}, and hence the inner product of r_i and r_j is 0. The only case that remain to be considered is when one of i or j is equal to 1 and the other one is in $\{(n+1)/2+1, \ldots, n\}$. In this case also the weight of $r_i \oplus r_j$ is 2, $wt(r_i), wt(r_j)$ are odd and $wt(r_i) = wt(r_j)$. Hence the inner product of r_i and r_j is 0. Thus the rows are pairwise orthogonal and B_n is nonsingular. □

Proposition 14. *For odd n, let f be an n-variable function constructed by Theorem 9. Then for each row r_i of B_n, $W_f(r_i) = 0$.*

Proof. Let $n = 2k+1$. Here we only show $W_f(r_1) = 0$ for $n \equiv 3 \bmod 4$, the other cases being similar. In this case r_1 represents the linear function in $L(2k+1)$ which is nondegenerate on all the variables $X_1, \ldots, X_k$. Let this function be l. Then we can write $l = \lambda^{2^{k+1}}$ (the string λ concatenated 2^{k+1} times), where λ is in $L(k)$ and is nondegenerate on all the variables $X_1, \ldots, X_k$.

We show that $wd(f, l) = 0$. Write f as a concatenation $f_1 f_2 \ldots f_p$, where $p = 2^{(n+1)/2}$. For $i \neq 1, p/2, p/2+1, p$, we must have $wd(f_i, \lambda) = 0$, since f_i is a linear function different from λ or λ^c. Therefore,

$$wd(f, l) = wd(f, \lambda^{2^{k+1}}) = wd(f_1, \lambda) + wd(f_{p/2}, \lambda) + wd(f_{(p/2)+1}, \lambda) + wd(f_p, \lambda).$$

Note that f is of the form $xyzx^c yz^c$ in the proof of Theorem 9. Hence comparing to the expression $f_1 f_2 \ldots f_p$ we have $f_1 = x$, $f_{p/2} = z$, $f_{(p/2)+1} = x^c$ and $f_p = z^c$. Hence

$$wd(f, l) = wd(x, \lambda) + wd(z, \lambda) + wd(x^c, \lambda) + wd(z^c, \lambda) = 0. \qquad \square$$

Using Propositions 13 and 14 and Theorem 9, we get the following result. Also the linear transformation does not change the number of values of Walsh spectrum. Thus, from Corollary 10, we get the result on the Walsh spectrum.

Theorem 15. *For odd $n \geqslant 7$, it is possible to construct 1-resilient, degree $(n-2)$ functions in Ω_n with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ having a five valued Walsh spectrum $\pm 2^{(n+1)/2}, 0, 2^{(n+1)/2} - 8, -8$.*

4.1. Higher order resiliency

Now we show how to extend the construction of the previous section to construct m-resilient maximum degree functions. For this we first recapitulate the construction from [10]. Let Q, R be operators ($Q, R : \Omega_n \times \Omega_n \to \Omega_{n+1}$) defined as follows.

For $f(X_n,\ldots,X_1), g(X_n,\ldots,X_1) \in \Omega_n$,

$$Q(f(X_n,\ldots,X_1), g(X_n,\ldots,X_1)) = F(X_{n+1},\ldots,X_1)$$
$$= (1 \oplus X_{n+1}) f(X_n,\ldots,X_1) \oplus X_{n+1} g(X_n,\ldots,X_1),$$

$$R(f(X_n,\ldots,X_1), g(X_n,\ldots,X_1)) = F(X_{n+1},\ldots,X_1)$$
$$= (1 \oplus X_n) f(X_{n+1}, X_{n-1},\ldots,X_1) \oplus X_n g(X_{n+1}, X_{n-1},\ldots,X_1).$$

For $1 \leqslant i \leqslant n+1$, this construction can be extended as

$$Q_i(f(X_n,\ldots,X_1), g(X_n,\ldots,X_1)) = F(X_{n+1},\ldots,X_1)$$
$$= (1 \oplus X_i) f(X_n,\ldots,X_{i+1}, X_{i-1},\ldots,X_1) \oplus X_i g(X_n,\ldots,X_{i+1}, X_{i-1},\ldots,X_1).$$

That is, $Q_{n+1} = Q$ and $Q_n = R$. It is easy to see that the operators Q_i are equivalent to each other under suitable permutations of the input variables. First we state the following result on the operator Q from [10].

Theorem 16 (Maitra and Sarkar [10]). *Let f be an n-variable, m-resilient degree d function having nonlinearity x. Define $F(X_{n+1},\ldots,X_1)$ to be an $(n+1)$-variable function as*

$$F(X_{n+1},\ldots,X_1) = Q(f(X_n,\ldots,X_1), a \oplus f(b \oplus X_n,\ldots,b \oplus X_1),$$

where, $a,b \in \{0,1\}$ and if m is even $a \neq b$ and if m is odd, $a = 1$ and b can be either 0 or 1.

Then $F(X_{n+1}, X_n,\ldots,X_1)$ is an $(m+1)$-resilient, degree d function having nonlinearity $2x$.

One can extend Theorem 16 as follows (see also [1]).

Theorem 17. *Let f be an n-variable, m-resilient degree d function having nonlinearity x. Define $F(X_{n+1},\ldots,X_1)$ to be an $(n+1)$-variable function as*

$$F(X_{n+1},\ldots,X_1) = Q_i(f(X_n,\ldots,X_1), a \oplus f(b \oplus X_n,\ldots,b \oplus X_1),$$

where, $a,b \in \{0,1\}$ and if m is even $a \neq b$ and if m is odd, $a = 1$ and b can be either 0 or 1.

Then $F(X_{n+1}, X_n \ldots, X_1)$ is an $(m+1)$-resilient, degree d function having nonlinearity $2x$. Moreover, if the Walsh spectrum of f is k valued then the Walsh spectrum of F is also k valued.

Proof. From Theorem 16, this is true for $Q_{n+1} = Q$. Any of the operators Q_i can be expressed as a composition of Q_{n+1} and a suitable permutation of the input variables.

The permutation of input variables preserves the resiliency, algebraic degree and nonlinearity. Thus the result is true for any operator Q_i.

Next we prove the stated property of the Walsh spectrum. Note that F can be represented by a binary string of length 2^{n+1}. Also, if we consider the operator $Q_{n+1}=Q$ then F has one of the form ff^c, ff^r or ff^{rc}, where f is a represented by a binary string of length 2^n. Let $\tau\in\{r,c,rc\}$, then F has the form ff^τ.

We compute the distance of F to an arbitrary linear function λ in $L(n+1)$. Note that λ can be written as ll or ll^c for some $l\in L(n)$. Now,

$$d(F,\lambda)=d(f,l)+d(f^\tau,l)=d(f,l)+d(f,l^\tau)$$

or

$$d(F,\lambda)=d(f,l)+d(f^\tau,l^c)=d(f,l)+d(f,(l^c)^\tau).$$

First note that if a linear function l is nondegenerate on even number of variables, then $l=l^r$ and if l is nondegenerate on odd number of variables then $l=l^{rc}$. Thus, if $d(f,l)=y$, then $d(F,\lambda)$ is either $2y$ or 0. So the Walsh spectrum of F contains either 0 or $2y$, where y is in the Walsh spectrum of f. Since f is resilient, by definition it is balanced and hence its Walsh spectrum contains the value 0 at the point $\bar{0}$. Hence the number of distinct values in the Walsh spectrum of F is same as the number of distinct values in the Walsh spectrum of f. □

We also need the following result for the construction purpose.

Theorem 18. *For even $n\geqslant 6$, it is possible to construct n-variable, 1-resilient functions with degree $n-2$ and nonlinearity $2^{n-1}-2^{n/2}$. Also these functions have five valued Walsh spectrum $\pm 2^{(n/2)+1}, 0, 2^{(n/2)+1}-8, -8$.*

Proof. Let f be an $(n-1)$-variable balanced function constructed by Theorem 7. Then $Q_i(f,f^c), Q_i(f,f^r)$ provide n-variable, 1-resilient functions having degree $n-2$ and nonlinearity $2nl(f)$. From Corollary 8, the Walsh spectrum contains five distinct values $\pm 2\times 2^{((n-1)+1)/2}=\pm 2^{(n/2)+1}, 0, 2\times(2^{((n-1)+1)/2}-4)=2^{(n/2)+1}-8, 2\times(-4)=-8$. □

The above results immediately suggest the following recursive procedure for constructing n-variable, m-resilient functions. The input to the procedure are two positive integers n and m with $1\leqslant m<n-2$.

(1) Let h be an $(n-m+1)$-variable, 1-resilient, degree $(n-m-1)$ function constructed using Theorem 18 or Theorem 15 accordingly as $(n-m+1)$ is even or odd.
(2) Theorem 17 is repeated $(m-1)$ times to obtain an n-variable, m-resilient, degree $(n-m-1)$ function f with nonlinearity $2^{m-1}nl(h)$.

Theorem 19. *The construction method given above constructs n-variable, m-resilient, degree $(n-m-1)$ functions with nonlinearity $nl(f)$, where*
(1) $nl(f)=2^{n-1}-2^{(n+m-2)/2}$ if $n-m+1$ is odd, and

(2) $nl(f) = 2^{n-1} - 2^{(n+m-1)/2}$ *if* $n - m + 1$ *is even.*
Moreover, if $n - m \geqslant 5$ *all these functions have five valued Walsh spectrum.*

Proof. Note that resiliency of the functions will be of order $1 + (m - 1) = m$. The algebraic degree does not change and remains constant at $(n - m - 1)$.

If $n-m+1$ is odd, $nl(f) = 2^{m-1} \times (2^{n-m} - 2^{(n-m)/2})$. In this case, the Walsh spectrum values will be $\pm 2^{(n+m)/2}, 0, 2^{(n+m)/2} - 2^{m+2}, -2^{m+2}$.

If $n - m + 1$ is even, $nl(f) = 2^{m-1} \times (2^{n-m} - 2^{(n-m+1)/2})$. Here the Walsh spectrum values will be $\pm 2^{(n+m+1)/2}, 0, 2^{(n+m+1)/2} - 2^{m+2}, -2^{m+2}$. □

5. Conclusion

Here we have considered the construction of resilient functions with maximum possible algebraic degree and high nonlinearity. We have shown how to algebraically modify the concatenation of two properly chosen Maiorana–McFarland bent functions to construct balanced (resp. 1-resilient) functions with degree $n - 1$ (resp. $n - 2$) and having bent concatenation nonlinearity. These are used as initial functions to certain recursive operators to construct higher order resilient functions having maximum possible degree and very high nonlinearity. Such functions have wide applications to stream cipher cryptography.

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation immune functions, in: J. Feigenbaum (Ed.), Advances in Cryptology—CRYPTO'91, Springer, Berlin, 1992, pp. 86–100.
[2] C. Carlet, Two new classes of bent functions, in: Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science, Vol. 765, Springer, Berlin, 1994, pp. 77–101.
[3] C. Carlet, Recent results on binary bent functions, in: International Conference on Combinatorics, Information Theory and Statistics, 1997.
[4] C. Carlet, P. Guillot, A characterization of bent functions, J. Combin. Theory, Ser. A 76(2) (1996) 328–335.
[5] P. Charpin, A. Canteaut, C. Carlet, C. Fontaine, Propagation characteristics and correlation-immunity of highly nonlinear boolean functions, in: Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science, Vol. 1807, Springer, Berlin, 2000, pp. 507–522.
[6] C. Ding, G. Xiao, W. Shan, in: The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, Vol. 561, Springer, Berlin, 1991.
[7] X. Guo-Zhen, J. Massey, A spectral characterization of correlation immune combining functions, IEEE Trans. Inform. Theory 34(3) (1988) 569–571.
[8] X. Hou, On the norm and covering radius of the first order Reed–Muller codes, IEEE Trans. Inform. Theory 43(3) (1997) 1025–1027.
[9] F.J. MacWillams, N.J.A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.
[10] S. Maitra, P. Sarkar, Highly nonlinear resilient functions optimizing Siegenthaler's inequality, in: M. Wiener (Ed.), Advances in Cryptology—CRYPTO'99, Lecture Notes in Computer Science, Vol. 1666, Springer, Berlin, August 1999, pp. 198–215.
[11] E. Pasalic, T. Johansson, Further results on the relation between nonlinearity and resiliency of Boolean functions, in: M. Walker (Ed.), IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, Vol. 1746, Springer, Berlin, 1999, pp. 35–45.

[12] N.J. Patterson, D.H. Wiedemann, The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276, IEEE Trans. Inform. Theory IT-29(3) (1983) 354–356.
[13] N.J. Patterson, D.H. Wiedemann, Correction to the covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276, IEEE Trans. Inform. Theory IT-36(2) (1990) 443.
[14] O.S. Rothaus, On bent functions, J. Combin. Theory, Ser. A 20 (1976) 300–305.
[15] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory IT-30(5) (1984) 776–780.